REMARKS

Applicants have now had an opportunity to carefully consider the Examiner's comments set forth in the Office Action of September 29, 2006.

Reconsideration of the Application is requested.

The Office Action

Claims 1-3, 5, 6 and 8-27 remain in the application.

Claims 21-27 stand rejected under 35 U.S.C. §101 as being directed to non-statutory subject matter.

Claims 1-3, 5, 6 and 8-27 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Meaney (US Patent Application Publication 20040139374) in view of Gilbertson (US Patent No. 6,594,785).

Claims 4 and 7 have been cancelled.

Rejections Under 35 U.S.C. § 101

Claims 21-27 have been amended to alleviate the 101 rejections. It is respectfully submitted that claims 21-27 are directed to statutory subject matter. Therefore, it is respectfully requested that the 101 ground of rejection of claims 21-27 be withdrawn.

Claims Distinguish over Prior Art

Claim 1 calls for among other elements: determining, based on a data poisoning policy, if the data poisoning event is to be acted upon. It is alleged in the Office Action that Gilbertson describes "determining, based on a data poisoning policy, if the data poisoning event is to be acted upon" in col. 27, lines 58-67. Applicants carefully reviewed the reference paragraph and did not find a description of "determining, based on a data poisoning policy, if the data poisoning event is to be acted upon. " The only relevant thing Gilbertson describes in col. 27, lines 58-67 is "the cache line state is set to poison, and the poison error indication is delivered to the operational requestor."

Further, Applicants cursory reviewed entire Gilbertson and did not find a description of "determining, based on a data poisoning policy, if the data poisoning event is to be acted upon." There is no mentioning of an overarching data poisoning policy anywhere in Gilbertson. To the contrary, claim 1 explicitly calls for a preset policy, e.g. a software pre-determined policy for how data poisoning events are to be handled, i.e. what specific actions are possible and what actions should be taken when the event occurs. The Operating System is allowed to control the policy, so that the tighter integration between hardware events and the event code is achieved.

Based at least on the above reasons, Applicants respectfully request the Examiner to remove this ground of rejection of claim 1. Neither Meaney, nor Gilbertson, taken singularly or in combination, disclose or suggest "determining, based on a data poisoning policy, if the data poisoning event is to be acted upon." It is therefore respectfully submitted that **claim 1 and dependent claims 2-3, 5-6, and 8-13** distinguish patentably and unobviously over Meaney and Gilbertson. If the Examiner maintains the rejection of claim 1 based on Gilbertson and/or Meaney, Applicants respectfully request the Examiner to point out exactly where in Gilbertson or in Meaney "determining, based on a data poisoning policy, if the data poisoning event is to be acted upon" is disclosed.

In addition to its relationship to claim 1, **claim 12** calls for among other elements: "determining whether or not to take immediate action on detection of a data-poisoning error comprises: setting a software visible control bit." It is alleged in the Office Action that Meaney describes "determining whether or not to take immediate action on detection of a data-poisoning error comprises: setting a software visible control bit" on page 6, para 55, lines 18-24. Applicants carefully reviewed para 55, lines 18-24, in which Meaney describes software visible bits to read the error information from the registers - "the present invention employs a novel ERR which permits firmware access to enable to central processor millicode to access the contents of the ERR during normal system operation. This enables a software driven method to access the UE tag status, determine which error types are present, isolate their origin, and take appropriate recovery action..." E.g., Meaney describes software reading hardware control bits to determine the next course of action

after the event has already occurred. According to claim 12, a software visible control bit is defined to indicate to hardware what action should be taken at the moment the event occurs. Neither Meaney, nor Gilbertson, taken singularly or in combination, disclose or suggest "determining whether or not to take immediate action on detection of a data-poisoning error comprises: setting a software visible control bit." It is therefore respectfully submitted that **claim 12** distinguishes patentably and unobviously over Meaney and Gilbertson taken singularly or in combination.

Claim 14 calls for among other elements: the operating system to implement a policy to determine if a particular data poisoning event is to be acted upon or not. The arguments above regarding claim 1 are equally applicable here. It is therefore respectfully submitted that **claim 14 and dependent claims 15-20** distinguish patentably and unobviously over Meaney and Gilbertson taken singularly or in combination.

Claim 21 calls for among other elements: determining, based on a data poisoning policy, if the data poisoning event is to be acted upon. The arguments above regarding claim 1 are equally applicable here. It is therefore respectfully submitted that **claim 21 and dependent claims 22-23** distinguish patentably and unobviously over Meaney and Gilbertson taken singularly or in combination.

Claim 24 calls for among other elements: determining, based on a data poisoning policy, if the data poisoning event is to be acted upon. The arguments above regarding claim 1 are equally applicable here. It is therefore respectfully submitted that **claim 24 and dependent claims 25-27** distinguish patentably and unobviously over Meaney and Gilbertson taken singularly or in combination.

CONCLUSION

For the reasons detailed above, it is submitted that all claims remaining in the application **(claims 1-3, 5, 6, and 8-27)** are in condition for allowance. The foregoing comments do not require unnecessary additional search or examination.

No additional fee is believed to be due for this Amendment. However, the undersigned attorney of record hereby authorizes charging of any necessary fees, other than the issue fee, to the Deposit Account No. 22-0261.

If the Examiner finds a personal contact advantageous to the disposition of this case, the Examiner is invited to call Marina Zalevsky, at telephone number 202-344-4975.

Dated: 11/28/2006

Respectfully submitted,

By _____

James R. Burdett
Registration No.: 31,594
Marina V. Zalevsky
Registration No.: 53,825
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)

::ODMA\PCDOCS\DC2DOCS1\794308\1